UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,909	04/06/2006	Vincent Carlier	4005-0277PUS1	7126

77032 7590 05/11/2009

Joe McKinney Muncy
PO Box 1364
Fairfax, VA 22038-1364

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
05/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/574,909	CARLIER ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 26 January 2009 has been noted and made of record.

2. Claims 1-10 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see page 5, filed 26 January 2009, with respect to the rejections made under 35 U.S.C. § 101 have been fully considered and are persuasive. The 35 U.S.C. § 101 of claims 1, 2, 4, and 5 has been withdrawn.

4. Applicant's arguments with respect to the prior art rejections filed on 26 January 2009 have been fully considered but they are not persuasive.

5. The applicant argues that Schwan does not disclose protecting an algorithm before it is introduced into a device. The examiner agrees. Schwan was cited to disclose the underlying claimed hardware. The examiner held that it would have been obvious to one of ordinary skill to implement the factoring to introduce the algorithm into the hardware of Schwan.

6. The applicant appears to argue that the factoring discussed below was inherent in Schwan. The examiner made no such assertion. The examiner presented evidence (Rajasekaran) to show that factoring was a well-known and commonly practiced technique. The examiner argued that the security features claimed by applicant are inherent in the known technique of factoring, specifically factoring a cryptographic equation in order to protect said equation prior to being implemented on a computer. The examiner held that it would have taken routine skill in the art to factor a complex polynomial into at least two quadratics, transport the at least two quadratics to a device, recombine the at least two quadratics, and implement the recombined polynomial on a processor. The combination of factoring with the introduction of an encryption

algorithm into a device appears to combine two known techniques to yield predictable results. As such the claim would have been obvious to one of ordinary skill, and the rejection is maintained.

7. See further rejections set forth below.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-4 and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 2004/0187035 A1 to Schwan et al., hereinafter Schwann, in view of known techniques.

10. As per claims 1 and 6, factoring is a technique taught to simplify complex polynomial equations. Factoring polynomials into quadratics, or simpler equations of at least a second degree (i.e. x^2), is known. U.S. Patent No. 4,922,539 to Rajasekaran et al., hereinafter Rajasekaran, discloses using the Bairstow technique for factoring polynomials with real coefficients into a set of quadratic polynomials for speech recognition (column 5, line 58 to column 6, line 14). The Applicant claims factoring a cryptographic equation in order to protect said equation prior to being implemented on a computer. MPEP 2112(I) states that the claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. See also *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977). In other words, the fact that the Applicant has found that factoring can be used to protect a cryptographic equation does not make the claim patentably distinct since factoring of complex polynomials has been well-known and commonly practiced in at least the

field of speech recognition since 1990. Recombining equations to form polynomials is also well-known and commonly practiced. This technique is typically taught in high school algebra on a much more basic level, such as $5(x - 1)(x + 2)(x - 3)(x + 4) = 5x^4 + 10x^3 - 65x^2 - 70x + 120$. One of ordinary skill would clearly be able to recombine several quadratic equations to reform the original polynomial. As noted in the previous Office Actions, Schwann teaches implementing an cryptographic algorithm n a processor (paragraphs 0002, 0010, 0015).

11. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the known techniques of factoring a complex polynomial, recombining said quadratics that were factored, and using said complex polynomial to introduce an encryption algorithm to a device, since it has been held that it only requires routine skill in the art to combine known elements to yield a predictable result. See MPEP § 2141(III); see also *KSR International Co. v. Teleflex Inc.*, 550 USPQ2d 1385 (2007).

12. Regarding claims 2 and 7, Schwan teaches the step of storing the encryption algorithms in the form of a configuration file that is loaded into a memory associated with the processor unit (paragraph 0002, i.e. updating the control program, programming the control unit to a customer and application needs, modify the functional and performance range of the control unit, reprogramming the control unit).

13. With regards to claims 3 and 8, Schwan teaches wherein the memory and the programmable processor unit are associated with an eraser member serving, in the event of an intrusion into the device, to erase the processor unit, and to erase the memory containing the

configuration file when the configuration is present in said memory (paragraph 0013, i.e. encryption algorithm is erased and/or destroyed after the housing is opened (the intrusion)).

14. Regarding claims 4 and 9, Schwan discloses the use of DES (paragraph 0013). As noted above DES combines more than two initial polynomials in order to obtain combined polynomials. DES also includes a function f_k and f_k^{-1}. This is supported by the disclosure of DES in **Cryptography and Network Security, Principles and Practices**, by William Stallings, hereinafter Stallings. Specifically, Stallings discloses the function f_k on at least page 61, or the initial permutation as disclosed on page 57. Stallings goes on further to discuss on page 57 the inverse initial permutation towards the end of the cryptographic calculation. Therefore Schwan teaches the step of combining each combined polynomial (Q_k) with a function (f_k), and of combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}) in his disclosure of DES.

15. Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwan in view of known techniques as applied above and in further view of **Applied Cryptography, Protocols, Algorithms, and Source Code in C**, by Bruce Schneier, hereinafter Schneier.

16. With regards to claims 5 and 10, Schwan does not teach wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the initial permutation, or claimed function f_k, be a linear function, since Schneier states at page 271 that the initial permutation is used to transpose the input block of

data, and as such a linear function would make it easier to transpose the input block and load the plaintext and ciphertext into a DES chip in byte-sized pieces.

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

19. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

21. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

22. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf